REMARKS

Claims 1-6, 8-12, and 14-23 are pending. No claim amendments are made with this response. Reconsideration of the application is respectfully requested based on the following remarks.

I. REJECTION OF CLAIMS 1-6, 8-12, and 14-23 UNDER 35 U.S.C. § 103(a)

Claims 1-6, 8-12, and 14-23 were rejected under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. US 7,003,118 B1 Yang et al. (Yang) in view of U.S. Patent No. US 6,418,130 B1 Cheng et al. (Cheng). Withdrawal of the rejection is respectfully requested for at least the following reasons.

i. Neither Yang nor Cheng teach a security system that is adapted to employ an initial random data string from the outgoing data to begin encryption..., as recited in independent claims 1 and 15.

Independent claim 1 recites a network interface system that is adapted to obtain initialization vector information from the host system and provide the initialization vector information to the security system, *wherein the security system is adapted to employ an **initial random data string** **from the outgoing data** which is used in the initialization vector (See, in one non-limiting example, IV 226 of outgoing data frame 200 of Fig. 1F, and IV INFO 191 of Fig. 1A) to begin encryption before security association information has been retrieved by the security system.*

The Office Action dated 11/16/2009 (see page 4, paragraph 5 to page 5 paragraph 1) admits that Yang does not teach *"the security system is adapted to employ an **initial random data string from the outgoing data** to begin encryption before security association information has been retrieved by the security system."*

In addition, Cheng also fails to teach using an ***initial random data string from the outgoing data to begin encryption***, but instead relies upon "*reusing **previously established security associations** to support these newly formed connections between the MU (mobile unit) and SU_{k+1}. By reusing these previously established*

security associations, the MU and SU_{k+1} need not go through the time consuming task of renegotiating the security associations (SA's) each time the MU changes it's point of connection (e.g., undergoes hand-over) within the administrative domain." (Column 3, lines 53-61 of Cheng).

Thus, it is apparent that to **re-use an SA**, Cheng must **first** have previously negotiated (retrieved) an SA, for it to then be **re-used** in a subsequent hand-over (from one SU to another). By contrast, the security system of the present invention *is adapted to employ **an initial random data string** from the outgoing data to begin encryption before security association information has been retrieved by the security system."* The **re-used SA** of Cheng is clearly not **an initial random data string** as recited in independent claims 1 and 15.

Thus, neither Yang nor Cheng disclose the features recited in claims 1 and 15.

Further, Cheng fails to teach that the *initial random data string is obtained **from the outgoing data.*** Instead, Cheng teaches ***re-using*** the *previously established security associations, after a hand-over, or after an MU has become disassociated to avoid the time consuming task of renegotiating the security associations*. (Column 3, lines 53-61, and Column 4, lines 18-38 of Cheng). Thus, the **previously negotiated SAs** of Cheng are obtained **from the MU or SU**, and are not obtained ***from the outgoing data**, such as an initial random data string which is used for the initialization vector information.*

Thus, two clear differences between Cheng and the present invention are:

1.) the present invention utilizes an ***initial random data string*** in order to permit encryption to begin before retrieving an SA, while by contrast, Cheng must first establish an SA in a first phase I, before a second SA negotiation and subsequent encryption in a second IPsec phase II [Cheng paragraph 1:43-60], and

2.) the present invention obtains the *initial random data string **from the outgoing data***, while by contrast, the **previously negotiated SAs** of Cheng are obtained **from the MU or SU.** This achieves a clear advantage for the present invention, particularly

as Cheng states: it is a *time consuming task of renegotiating the security associations.* Therefore, the time consuming initial negotiation of the SAs of Cheng need not delay the encryption of the present invention achieved using the ***initial random data string*** obtained ***from the outgoing data*** as recited in independent claims 1 and 15.

Thus, neither Yang nor Cheng disclose the features recited in claims 1 and 15. Therefore, Applicant respectfully submits that independent claims 1 and 15, and the claims which depend therefrom, respectively, are non-obvious and therefore patentable over Yang in view of Cheng. Withdrawal of this rejection is therefore respectfully requested.

ii. Neither Yang nor Cheng teach a security system that is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system, as recited in independent claims 1 and 15.

Independent claim 1 further recites a network interface system that is adapted to obtain initialization vector information from the host system and provide the initialization vector information to the security system, ***wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.***

Again, the Office Action dated 11/16/2009 (see page 4, paragraph 5 to page 5 paragraph 1) admits that Yang does not teach *"the security system is adapted to employ an initial random data string from the outgoing data to begin encryption* ***before security association*** *information* ***has been retrieved*** *by the security system."*

In an attempt to remedy this deficiency, the Office Action dated 11/16/2009 (see page 3, paragraph 1, line 7) incorrectly summarizes that Cheng describes in [paragraph 1:30-60 and Fig. 4] that "*encryption can be done prior to establishing phase II / IPsec SA attributes.* However, this is a misinterpretation, because Cheng describes in [paragraph 1:48-60] that Cheng has already negotiated ISAKMP SA's in Phase 1

before negotiating IPsec SA's and subsequent encryption in Phase 2, as a Phase 2 always follows Phase 1. That is, the two phases are not independent in Cheng, as Cheng reiterates several times: *"phase 1 negotiation and phase 2 negotiation **must be accomplished**"* [paragraph 7:7-11], and "***must conduct phase 2**"..."must renegotiate the IPsec SA's*" in [paragraph 4:18-34]. Thus, Cheng teaches that a negotiated SA takes place in both phases 1 and 2 before encryption in phase 2 as indicated above, and that the two phases **must** both be accomplished.

Therefore, Cheng does not teach employing *an initial random data string from the outgoing data to begin encryption **before SA information has been retrieved** by the security system*, as recited in claims 1 and 15.

Further, Cheng relies upon "***reusing previously established security associations** to support these newly formed connections between the MU (mobile unit) and SU_{k+1}. By reusing these previously established security associations, the MU and SU_{k+1} need not go through the time consuming task of renegotiating the security associations (SA's) each time the MU changes its point of connection (e.g., undergoes hand-over) within the administrative domain.*" (Column 3, lines 53-61 of Cheng). Thus, in order to **re-use an SA**, Cheng must **first** have previously negotiated (retrieved) an SA, which can then be re-used in a subsequent hand-over (from one SU to another) or "*if the MU becomes disassociated from the administrative domain, for example, by being handed over to a SU which is not associated with the administrative domain*" (Column 7, lines 17-26 of Cheng). By contrast, the security system of the present invention *is adapted **to begin encryption before security association information has been retrieved**.*

That is, Cheng teaches a significantly different methodology, teaching that "*the MU establishes a connection with the SU in the administrative domain for **the first time**, wherein the Internet Key Exchange (IKE) negotiates to **establish an SA**...*", and "***the first time** a MU connects to any SU in a given administrative domain, an IKE phase 1 negotiation and an IKE phase 2 negotiation must be accomplished, thereby*

establishing *the ISAKMP* ***SA*** *and the IP$_{SEC}$* ***SA****s respectively.*" (Column 4, lines 18-28, and Column 7, lines 7-11 of Cheng). However, the security system of the present invention begins encryption before retrieving an SA, without having to wait for the time consuming task of negotiating the initial SA. (See, in one non-limiting example, Applicants' specification page 5, lines 27-29).

Thus, the clear difference between Cheng and the present invention is that Cheng must first establish an SA before it can be "re-used" to begin encryption in an IPsec phase II, while by contrast, the present invention begins encryption **before** security association information has been retrieved by the security system, employing an initial random data string from the outgoing data. Restating this difference, Cheng must first negotiate an SA before encryption, while in the present invention; encryption begins before retrieving an SA. This is a clear advantage, particularly as Cheng states: it is a *time consuming task of renegotiating the security associations.*

For example, and to illustrate this comparison, assume a cell phone or mobile unit (MU) needs to communicate 50 blocks of data with a first tower or first stationary unit (SU1). According to Cheng, the first time the MU is associated with SU1, the SA's are negotiated (established) in the usual time-consuming negotiation manner. Now upon communicating block 37 of the 50 blocks, let's assume the MU becomes disassociated with SU1 and must be handed-over to a second tower or second SU (SU2) to communicate the remaining data blocks 38 thru 50. According to the teaching of Cheng, the MU will then become associated with SU2 by re-using the *previously established security associations*, which in this case were established with SU1, to avoid the time consuming task of having to renegotiate the SA's as Cheng admits it did the first time. Then, in accordance with Column 6, lines 61-63 of Cheng, *in the last CBC block* (block 37), *prior to hand-over* to SU2, block 37 *is used as the initialization vector for encryption of the first IP packet* (block 38) *subsequent to hand-over.*

Thus, Cheng may be useful for re-using the *previously established security associations, after a hand-over, or after an MU has become disassociated to avoid the time consuming task of renegotiating the security associations*. However, to avoid

having to wait for this same time consuming task during the **initial negotiation** of the security associations and to immediately begin the initial encryption, the *security system* of the present invention *is adapted to employ an initial random data string from the outgoing data to begin encryption* ***before SA information has been retrieved*** *by the security system*, as recited in claims 1 and 15.

Thus, neither Yang nor Cheng disclose the features recited in claims 1 and 15. Therefore, Applicant respectfully submits that independent claims 1 and 15, and the claims which depend therefrom, respectively, are non-obvious and therefore patentable over Yang in view of Cheng. Withdrawal of this rejection is therefore respectfully requested.

II. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, GFP108US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600